MSC

Messerschmidt
Safety Consultants

www.mscrecon.com

Mississippi Office
601.297.6598 | 205.444.0071
6068 Highway 98,
Suite 1-144
Hattiesburg, MS 39402

Benjamin N. Smith
ACTAR #2270
Principal Technical Analyst
b.smith@mscrecon.com

Alabama Office
205.444.0071 | 205.444.0073 fax
2148 Pelham Parkway,
Bldg. 100-B
Pelham, AL 35124

William F. Messerschmidt
MPA, ACTAR #1372
Principal Technical Analyst
w.messerschmidt@mscrecon.com

Mr. Hicks,

The following summarizes our chip-level digital forensics into the damaged Sensing and Diagnostic Module (SDM) from a 2004 GMC Yukon VIN 1GKEC13Z04R289898.

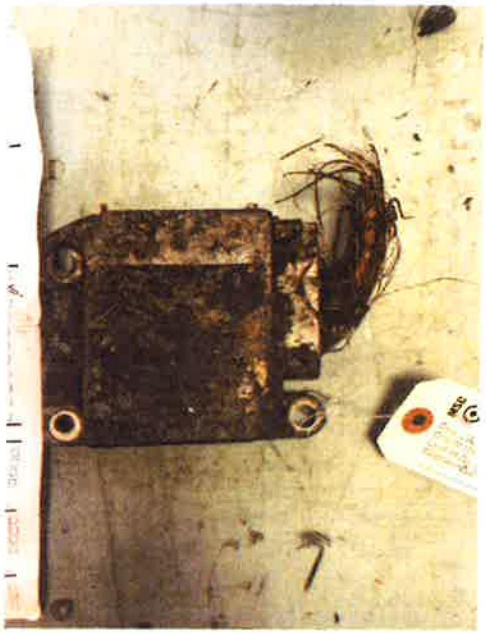

Figure 1: Subject SDM

Damage Analysis

Upon receiving the SDM, it was photographed and entered into our evidence intake system. The subject SDM was evaluated to determine the extent of damage. The outside case showed signs of extreme heat exposure. The Input/Output connectors and corresponding wiring harness was visibly melted, this made any attempts to back probe the connector impossible (Figure 2). Upon inspecting the underside of the module the sealant used to protect the printed circuit board (PCB) was visibly charred and appeared to have undergone chemical decomposition as a result of the heat (Figure 3). A corner section of sealant was scrapped away to evaluate any PCB damage due to heat (Figure 4). A visible inspection of the PCB determined the board began to delaminate due to extreme temperatures. At this time, it was determined the board could not be repaired.

EXHIBIT
tabbies
E

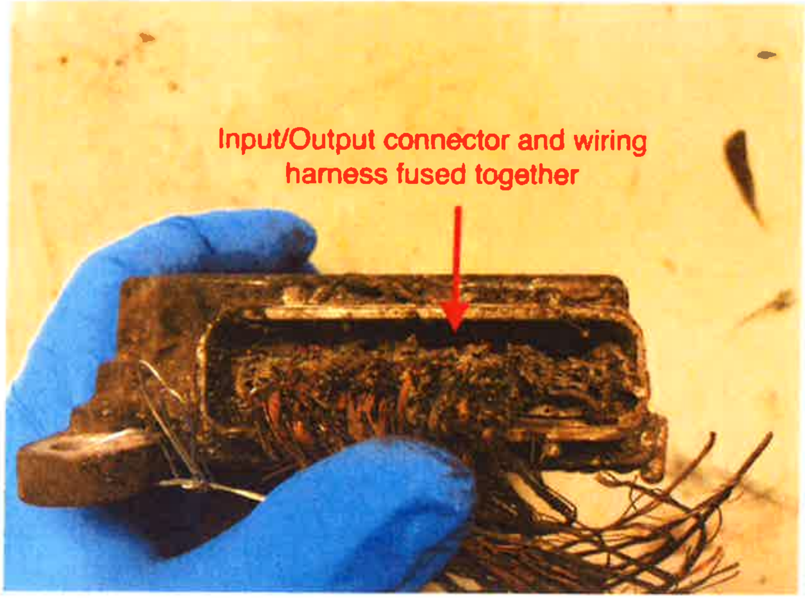

Figure 2: Shows fusion of Input/Output connector with wiring harness.

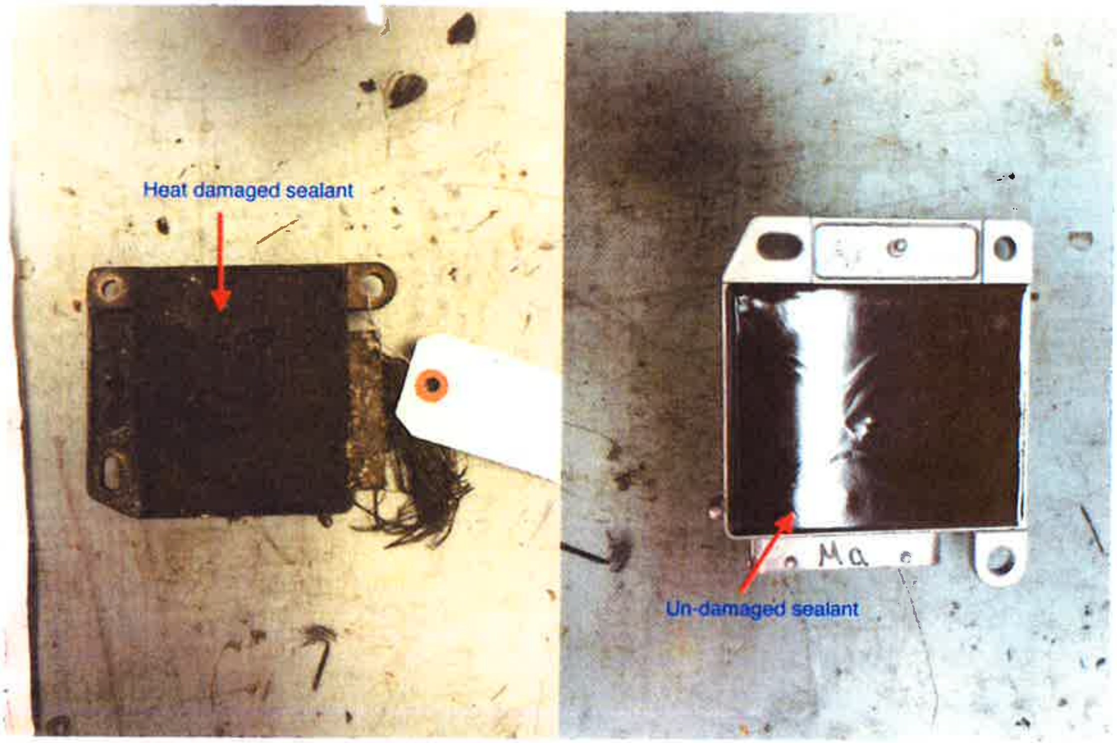

Figure 3: Shows a comparison between damaged and un-damaged sealant protecting PCB.

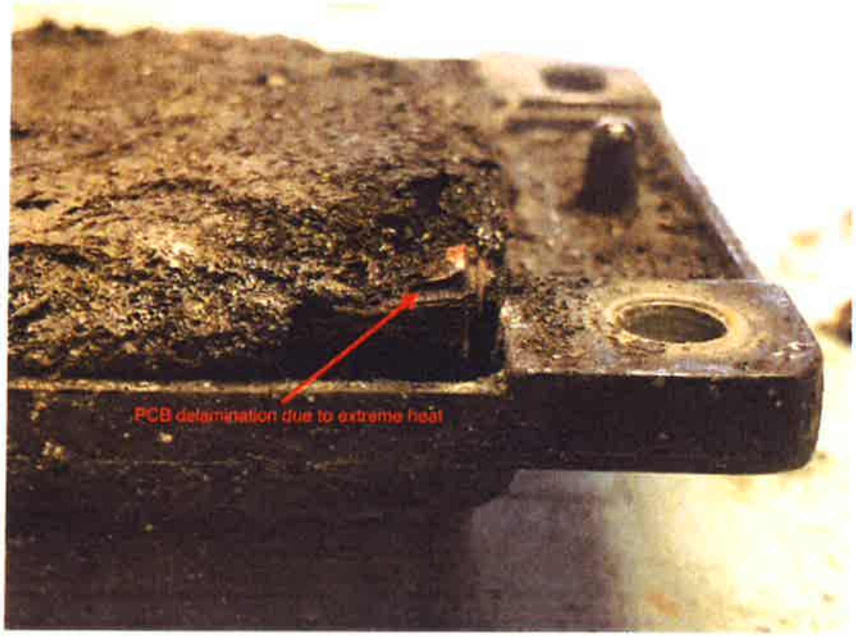

Figure 4: Shows the delamination of copper and substrate within PCB.

Component Identification

The PCB needed to be completely disassembled to identify and determine the status of any data bearing components. There were a number of surface mount devices (SMD) resistors and capacitors that subsequently became unsoldered due to heat on the underside of the PCB. Upon inspecting the top-side of the board there were 4 x 1500uF capacitors and 2 x 39uF capacitors that incurred heat damage of some type. There were also a number of integrated circuits (IC) that had become unsoldered from the PCB. Two components in particular stood out to be of interest, the larger component was suspected to be a microcontroller and the smaller component was suspected to be an EEPROM (Figure 5). In order to confirm, we proceeded to conduct a proof of concept on two surrogate modules.

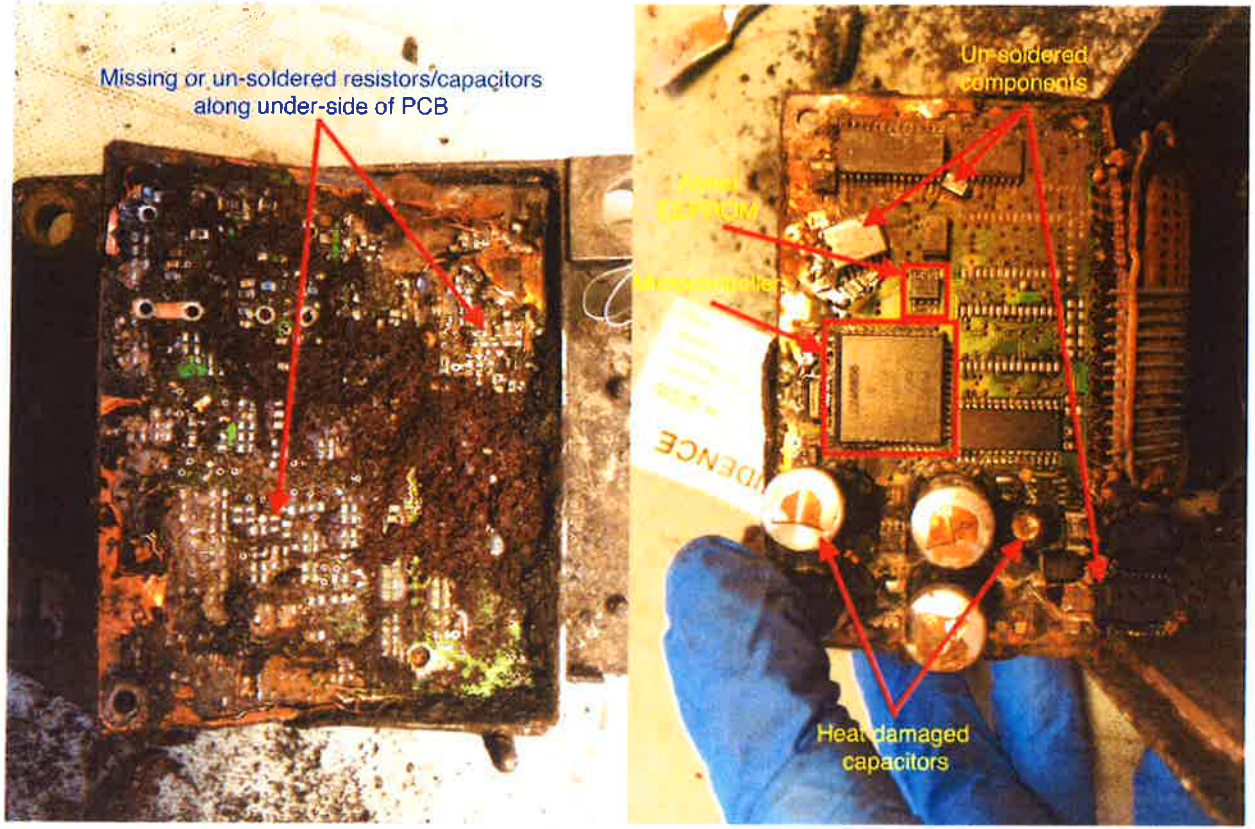

Figure 5: Shows damage to both sides of PCB and components.

Possible Solutions

There are two possible techniques that could be used to extract data from this SDM, one being more destructive than the other. The two techniques are JTAG and Chip-Swap.

JTAG Technique

Joint Test Action Group (JTAG) is an industry standard used for testing printed circuit boards (PCB) as they come off the manufacturing assembly line to ensure all the appropriate connections have been made and the device is working properly. JTAG forensics is a technique that uses that same process and involves connecting to the Test Access Ports (TAPs) on a PCB via solder and then uses a supported JTAG Box to instruct the processor to acquire the raw data stored on the connected memory chip to get a full physical image from the device. Once that image is acquired from the subject SDM, we could then write the image using the same process to a "new" surrogate SDM and download any/all data directly from there. This process is non-destructive.

This would usually be the first technique I would consider since it is typically non-destructive, but there are a few issues with this SDM that makes this technique not possible. The issues that we may run into using this method: The first is that the JTAG technique requires the ability to apply power to the SDM through the conventional Input/Output connector which in this case is melted and beyond repair. If the connector was repairable and we were able to apply power to the SDM then the concern was the delamination of the PCB and fire-induced damage to components/connections, this damage would make any attempt to connect to the processor unsuccessful. In which case the chip-swap technique was our only option.

Chip-swap Technique

Chip-swap forensics is the process in which a memory chip, in this case EEPROM, is removed from a damaged SDM and transplanted into a NEW working, surrogate SDM. Unlike JTAG, chip-off is a destructive process by nature. The concern was the fire may have caused damage to the EEPROM component itself. Testing done by Exponent Failure Analysis Associates of Toyota event data recorders revealed that some EEPROMs were capable of withstanding direct flame impingement between 13 and 28 seconds before the component developed cracks in the chip and lost functionality. With that knowledge, it is unlikely this EEPROM every received any type of direct flame impingement and was likely subjected to in-direct thermal stresses. The time duration was unknown but based on visible inspection of the chip there were no evident cracks or damage that would indicate the chip was non-functional.

Proof of Concept

Based on visible inspection and research of the subject SDM I suspected the crash data to be stored on a I^2C Serial EEPROM. The package format for this chip is an 8-lead Small Outline Integrated Circuit (SOIC). The following steps were taken to retrieve any/all data potentially stored on the subject SDM:

1. Two identical, surrogate SDMs were purchased to complete a proof of concept before any work began on the subject SDM. Both SDMs were downloaded to obtain a baseline and prove they were "new: containing zero recorded events.
2. These two SDMs were disassembled to confirm similar construction and architecture to the subject SDM. The disassembly of these two surrogate SDMs allowed a visible inspection of undamaged modules to ensure no important components had been damaged/lost from the subject SDM.
3. SDM A was placed on our event simulation device that simulates a known crash event and records subsequent crash data. After crash data was successfully saved to the SDM, it was downloaded again to verify crash data exists. Two events were created, Deployment with Maximum SDM Recorded Velocity Change -12.16 MPH and Non-Deployment with Maximum SDM Recorded Velocity Change -0.33 MPH. Keep in mind there is no recorded pre-crash data because the SDM was tested as a stand-alone and was not connected to any external CAN bus or sensors.
4. At this point, the identified Atmel EEPROM component was removed from SDM A and re-soldered to the one remaining "new" SDM B.

5. After successful transplant SDM B was downloaded to verify the simulated crash data had been transferred from SDM A in its entirety. All crash data had been transferred successfully. Two variables, Ignition Cycles at Investigation and Frontal Deployment Level Event Counter are both counters stored in the microcontroller. This data represented crucial data from the respective surrogate module that visibly showed the surrogate module was essentially "new" with no data to contaminate the chip swap process.
6. The identified and tested data-bearing EEPROM component was then removed from the subject SDM and transplanted to the surrogate SDM B and downloaded.

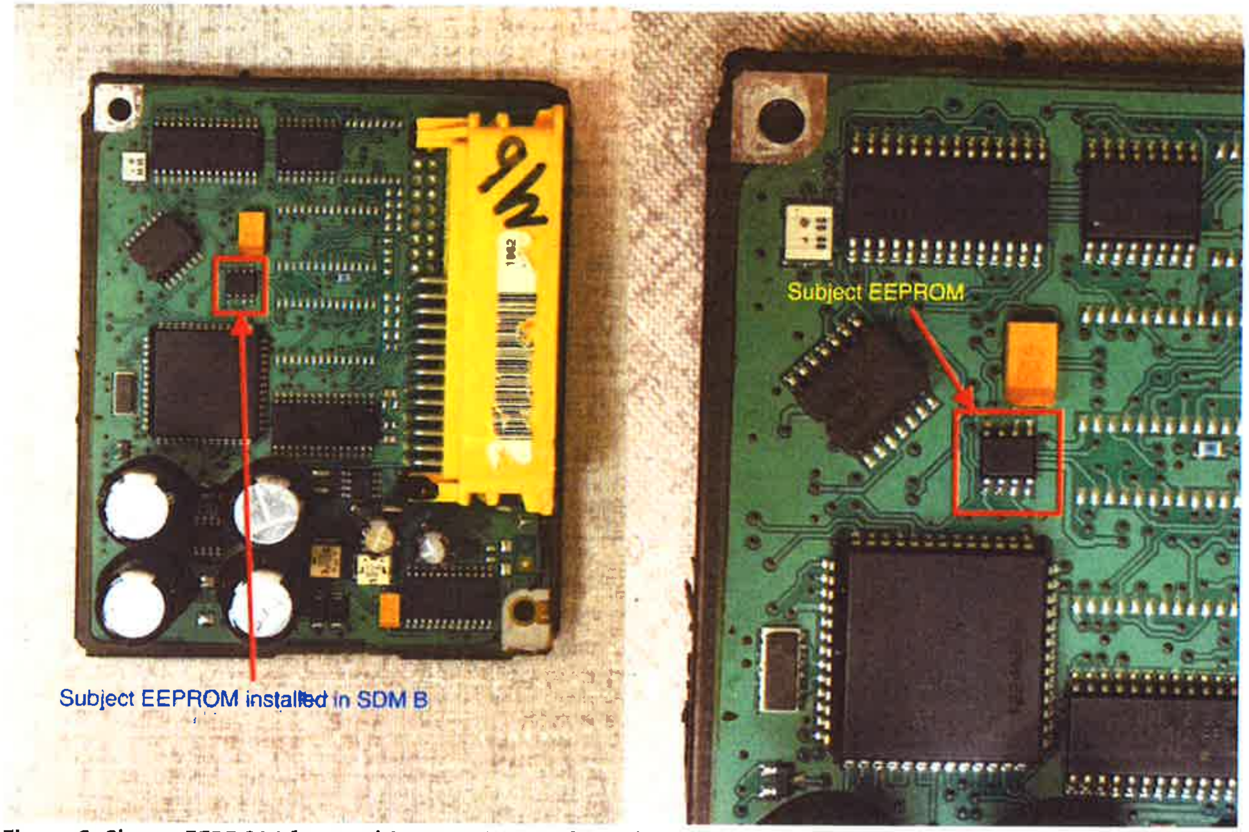

Figure 6: Shows EEPROM from subject SDM transplanted into surrogate SDM B.

Thanks,

Shanon Burgess